AMENDMENTS TO CLAIMS

Claim 1 (currently amended): A method for digitally signing a message, the method comprising:

providing a message digest (M_X, M_Z);

providing a modulus N of length n bits;

providing a number V in the ring Z_N, wherein for another number S in the ring Z_N, $V \cdot S^2 = 1$ in Z_N;

providing two numbers u and v, such that the following conditions are satisfied for u and v:

the sum of u and v is close to n;

u is greater than or equal to n/2; and

v is neither close to 0 nor close to n;

finding three numbers x, y, and z, such that the following conditions are satisfied for x, y and z:

$0 <= x < 2^u$;

$0 <= z < 2^v$; and

$(M_x + x)^2 - V \cdot y^2 = 4 \cdot (M_z + z)$ in Z_N;

~~solving the equation $(M_x + x)^2 - V \cdot y^2 = 4 \cdot (M_z + z)$ in Z_N to produce x, y, and z;~~ and

assigning a value comprising an ordered triple (x,y,z) as the signature (SIG) ~~as the signature~~ of (M_X, M_Z), ~~wherein SIG comprises (x,y)~~ thereby digitally signing the message.

Claim 2 (cancelled)

Claim 3 (currently amended): The method according to claim 1 and wherein the finding ~~solving~~ comprises the following:

a) choosing a first number α and a second number β in Z such that $0 \leq \alpha < \beta < 2^{k-1}$ 2^{n-u-1} and $\gcd(\alpha, \beta) = 1$ in Z;

b) choosing a third number γ in Z such that ~~2^{n-k-1}~~ $2^{u-1} \leq \gamma < $ ~~2^{n-k}~~ 2^{u} and $\beta \mid (\alpha \cdot N + \gamma)$ in Z;

c) setting a fourth number R equal to $(\alpha \cdot N + \gamma) / \beta$ in Z;

d) setting a fifth number T equal to $-(M_z \cdot R + M_x + R^{-1})$ in Z_N;

e) if $\beta = 1$ or $T < 8 \cdot \gamma$ (in Z), setting a sixth number U and a seventh number W equal to 0 and continuing with step k;

f) setting an eighth number D equal α^{-1} in Z_β;

g) setting a ninth number A equal to N / β in Z;

h) setting a tenth number B equal to $(T - 8 \cdot \gamma) / A$ in Z;

i) setting U equal to $B \cdot D$ in Z_β;

j) setting W equal to $U \cdot R$ in Z_N;

k) setting an eleventh number C equal to $(T - W) / \gamma$ in Z;

l) setting z equal to $U + \beta \cdot C$ in Z_N;

m) setting x equal to $T - z \cdot R$ in Z_N; and

n) setting y equal to $S \cdot (x + M_x + 2 \cdot R^{-1})$ in Z_N,

thereby producing x, y, and z.

Claim 4 (original): The method according to claim 3 and also comprising:

providing a trusted computation device and a non-trusted computation device,

wherein step d) comprises performing a computation in the non-trusted computation device.

Claim 5 (original): The method according to claim 4 and wherein the computation in the non-trusted computation device comprises a computation of R^{-1}.

Claim 6 (original): The method according to claim 5 and wherein the computation in the non-trusted computation device is protected from tampering by performing a blinding method in the trusted computation device.

Claim 7 (original): The method according to claim 6 and also comprising verifying a result of the computation in the non-trusted computation device.

Claim 8 (original): The method according to claim 3 and wherein step a) comprises screening α and β.

Claim 9 (original): The method according to claim 8 and wherein the screening comprises reducing α and β modulo 210.

Claim 10 (original): The method according to claim 9 and wherein the reducing α and β modulo 210 comprises:

computing gcd(210, (α mod 210), (β mod 210)) to produce a result; and

rejecting α and β and choosing another α and β if the result is not equal to 1.

Claim 11 (currently amended): The method according to claim 1 and wherein the finding ~~solving~~ comprises the following:

~~a) setting α equal to 0;~~

~~b) setting $\beta = 1$;~~

[[c]]a) choosing a first number γ such that ~~2^{n-k-1}~~ $2^{u-1} \leq \gamma < $ ~~2^{n-k}~~ 2^{u};

[[d]]b) setting a second number T equal to $-(M_z \cdot \gamma + M_x + \gamma^{-1})$ in Z_N;

[[e]]c) setting z equal to T / γ in Z;

[[f]]d) setting x equal to $T - z \cdot \gamma$ in Z_N; and

[[g]]e) setting y equal to $S \cdot (x + M_x + 2 \cdot \gamma^{-1})$ in Z_N,

thereby producing x, y, and z.

Claim 12 (currently amended): The method according to claim 11 and also comprising:

providing a trusted computation device and a non-trusted computation device,

wherein step [[d]]b) comprises performing a computation in the non-trusted computation device.

Claim 13 (original): The method according to claim 12 and wherein the computation in the non-trusted computation device comprises a computation of γ^{-1}.

Claim 14 (original): The method according to claim 13 and wherein the computation in the non-trusted computation device is protected from tampering by performing a blinding method in the trusted computation device.

Claim 15 (original): The method according to claim 14 and also comprising verifying a result of the computation in the non-trusted computation device.

Claim 16 (cancelled)

Claim 17 (new): The method according to claim 1 and wherein the method is implemented in a computing device.